UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

BCS

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/187,700	11/06/98	KOBAYASHI H	3408.62676

024978
GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO IL 60606

WM31/0509

EXAMINER	
NEWTON, G	
ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 05/09/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	09/187,700	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	Gregory Newton	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 November 1998* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
18) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other:

DETAILED ACTION

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Drawings

2. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Specification

3. The disclosure is objected to because of the following informalities:

The disclosure seems to be translated in an unclear manner. For example, consider lines 19 and 20 on page 2; "A ..storage medium such an optical disk is stored with the data.."

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 7 and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is not possible to examine claims 7 and 14 in their present form. It is unknown which group of passwords the other password belongs to, and the terms are not well-defined. It is unknown what differentiates the one password from the other passwords or password. However, a password is equivalent in many respects with a key, and therefore such encryptions, re-encrtyptions, and self-encrtyptions would be found to be taught in the Schneier reference, chapter 8. Claims 7 and 14 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 15 is rejected under 35 USC 102(b) as being unpatentable over Al-Salqan, (US 6,160,891).

7. Claim 15 recites a claim of a storage medium whereon encrypted data is stored by way of a key encrypted with a password. However, these disclosures can be found within the ABSTRACT of the Al-Salqan reference of note. Claim 15 is rejected.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-6, are rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan (US 6,160,891), and further in view of Dumas et al (US 6,199,163), or Schneier.

10. Claim 1 claims a method of writing a key, which has been encrypted with a password, to a storage medium, and then encrypting data to the storage medium using this key. Claim 1 also recites the inverse decrypting operation of this method.

However, we find these teachings in patent US 6,160,891 issued to Al-Salqan, Methods and Apparatus for Recovering Keys. In the ABSTRACT, as well as in other places in the published patent, Al-Salqan teaches of a key which is encrypted by using a key password, which is then stored, and accessible by way of the inverse means. He teaches in column 2 lines 1-3 that the message data is then encrypted with the key data. However, he doesn't mention the destination of this encrypted data, but it would be obvious to one of ordinary skill in the art that a natural destination of the data would be a storage device. In fact, we find these teachings about securing data on a storage

be a storage device. In fact, we find these teachings about securing data on a storage device in US 6,199,163 by Dumas et al, Hard Disk Password Lock. Here, within the ABSTRACT, as well as throughout the patent publication, Dumas teaches of a device which provides an encryption circuit for encrypting and decrypting data as it travels to and from a hard disk, where the disk cannot be read without the user supplied password and a similar encryption circuit. Furthermore, Dumas even teaches in column 4 in the Detailed Description of a Preferred Embodiment where an encryptor receives encoded private information (passwords) and encrypts the key. (It is also found in Schneier, section 8.7, called STORING KEYS, where he mentions regenerating keys from an easy to remember password when they are required, and that ideally a key should never appear unencrypted outside the encryption device.) Therefore, we see that by the teachings of Al-Salqan and further in view of Dumas, that the claim 1 of the disclosure would have been obvious to one of ordinary skill in the art at the time of the disclosure, and furthermore that one of ordinary skill in the art would be motivated to safeguard stored data as taught by Dumas. Claim 1 is rejected.

11. Claim 2 recites the method of claim 1, protecting storage medium data, but wherein the generation of keys is done per logic sector on the storage medium. However, it is found in the Dumas reference of note that this method of key generation per logic sector is previously taught. In the second paragraph of column 4, Dumas teaches that the encryption to storage medium method continues until the end of a sector is reached, and where a new sector always begins at the beginning of the

password. Consequently, and in view of the rejection of claim 1, it is noted that the generation of keys per logic sector would have been obvious to one of ordinary skill in the art at the time of the disclosure. Therefore, and in accordance with the rejection of claim 1, claim 2 is rejected.

12. Claim 3 recites the method of claim 2, but which is done when writing the data. However, it is noted that this method is claimed in claim 7 of the Dumas reference of note, where he teaches the method of encrypting data as it travels from the CPU to said mass storage device. In view of this teaching, and further in view of Dumas' teachings concerning the encryption of data per logic sector as discussed above with regard to the rejection of claim 2, it is noted that it would be obvious to one skilled in the art that encrypting data as it travels from the CPU to the said mass storage device is equivalent to the disclosures of claim 2, but occurs when writing the data to the storage device. Therefore, and in accordance with the rejections of claim 2 and claim 1 above, claim 3 is rejected.

13. Claim 4 recites the storage medium data protecting method according to claim 1, but wherein the key is generated from random data. We refer here to teachings of B. Schneier, Applied Cryptography, 1996. In chapter 8.1, called "Generating Keys", is found the section called "Random Keys". Here is found the teaching of assembling key data from random data. Therefore, in view of the rejection of claim 1, and further in view of these teachings within Schneier, note is taken that someone with ordinary skill in

the art would find it obvious to be motivated to make a key out of random data if so desired. There are also technical questions which are well known in the art about the possibility of obtaining true random data. Therefore, and in accordance with the rejection of claim 1, claim 4 is rejected.

14. Claim 5 claims the storage medium data protecting method according to claim 1, but further comprising decrypting the key data with the password and then re-encrypting this key with a new password. This method is found to be taught within the Al-Salqan reference, Methods and Apparatus for Recovering Keys. Al-Salqan teaches in column 5, second paragraph, that in one embodiment of the invention a user may not only assign a key password to a key, but may update a key password. In fact, one with ordinary skill in the art would naturally be motivated to include means for changing the password, which would include means of bringing the key out of encryption using the old password and then re-encrypting the key again with the new password. Therefore, and in accordance with the rejection of claim 1, claim 5 is rejected.

15. Claim 6 claims the method of claim 1, but where encrypting the file to storage is done by a plurality of passwords. Observe that this is taught in the disclosures of Al-Salqan of the references listed. At the top of column 4, Al-Salqan teaches of the encryption of the key by means of a plurality of private information data, including social security number, mother's maiden name, etc. In other words, these constitute a plurality of passwords used to encrypt the key. Also, the disclosed step of decoding the

key data with a designated password is just the inverse operation, which would have to be included in order to access the key. And so, it is found that these disclosures of claim 6 would be found obvious to one skilled in the art who would be motivated to employ the methods of either Al-Salqan or Dumas, noted in the references. Therefore, and in accordance with the rejection of claim 1, claim 6 is rejected.

16. Claims 8-13 are apparatus implementations of the methods recited in claims 1-6, and are rejected in view of the same prior art of record and according to the same rationale.

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 6,094,721, Eldridge et al, METHOD AND APPARATUS FOR PASSWORD BASED AUTHENTICATION IN A DISTRIBUTED SYSTEM, filed 10/77.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory Newton, whose telephone number is 703-305-1373. The examiner can normally be reached on M-F 9-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on 703-308-7791. The fax phone numbers for

the organization where this application or proceeding is assigned are 703-308-9051 for regular communications and 703-308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Gregory A Newton
May 4, 2001

TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

380/277

2001-03-19 18:31:28

S49

U

USPT

380/277

2001-03-19 18:31:26

S48

U

USPT

(key adj3 password) and encrypt

2001-03-19 18:03:32

S47

U

USPT

(key adj3 password) and re-key and encrypt

2001-03-19 18:03:16

S46

U

USPT

(key adj3 password) and re-key

2001-03-19 18:02:19

S45

U

USPT

key adj3 password

2001-03-19 18:01:32

S44

U

USPT

key.ti. and encrypt.ti.

2001-03-19 17:56:41

S43

U

USPT

"password encrypts key"

2001-03-17 20:13:59

S42

U

USPT

"encrypting data".ti. and "encrypted key".ti.

2001-03-17 20:10:56

S41

U

USPT

"encrypting data".ti.
2001-03-17 20:10:11

S40
U
USPT
"encrypt$ data".ti.
2001-03-17 19:51:24

S39
U
USPT
("encrypting data".ti.) and
"encrypting key"
2001-03-17 19:48:12

S38
U
USPT
("encrypting data".ti.) and
"encrypted key"
2001-03-17 19:47:50

S37
U
USPT
("encrypting data".ti.) and
"encrypt$ key"
2001-03-17 19:47:15

S36
U
USPT
"encrypting data".ti.
2001-03-17 19:45:23

S35
U
USPT
"password encrypts key"
2001-03-17 19:37:04

S34
U
USPT
"encrypting key with password"
2001-03-17 19:36:28

S33
U
USPT
"encrypting key".ti.
2001-03-17 19:33:00

S32
U
USPT

"encrypt said key with password"
2001-03-17 19:30:37

S31
U
USPT
"encrypt $ key with password"
2001-03-17 19:30:12

S30
U
USPT
"encrypt key with password"
2001-03-17 19:29:40

S29
U
USPT
"encrypted key".ti. and
password.ti.
2001-03-17 19:28:50

S28
U
USPT
"encrypted key".ti.
2001-03-17 19:21:02

S27
U
USPT
"encrypted key"
2001-03-17 19:06:33

S26
U
USPT
encrypted and key and password
and data
2001-03-17 19:05:37

S25
U
USPT
encrypted and key and password
2001-03-17 19:04:37

S24
U
USPT
encrypted and key
2001-03-17 19:04:07

S23
U
USPT
encrypted key

USPT

(((713/185)!.CCLS.))

2001-03-26
13:15:17

S55

U

USPT

(((713/183)!.CCLS.))

2001-03-26
12:41:53

S54

U

USPT

((713/182)!.CCLS.)

2001-03-26
12:39:28

S53

U

USPT

encrypt adj key adj3 password

2001-03-20
16:10:39

S52

U

USPT

encrypt adj key

2001-03-20
16:09:31

S51

U

USPT

encrypt key

2001-03-20